6.915 Computer and Network Security **Fall Term, 1995**

Lecture 22 : November 28, 1995

Lecturer: Ron Rivest *Scribe: Gillian Elcock*

1 Outline

The main topic of this lecture is Firewalls. The outline is as follows:

- Packets, TCP/IP
- Packet filters
- Application gateways

Some recommended reading for this topic is the book *Firewall and Internet Security* by Cheswick and Bellovin.

2 Function of Firewalls

There are different approaches to making a computer system secure from attacks from the Internet. One is to try to make sure that all of the computers are secure, i.e. to make sure that users pick secure passwords, to apply security patches, etc. However, this is usually hard to do.

Another approach is to install a monitor or gateway, separating the internal network from the Internet. This is called a *firewall* (see figure 1). All communications between the Internet and the internal network must go through the firewall, which does a security check on them. The internal machines may be maintained casually, but the firewall will have very strict security codes. Firewalls are also useful for keeping logs of transactions between the Internet and the network, which could be used for intrusion detection.

The usual policy for a firewall is *"Everything not expressly permitted is prohibited."*

Firewalls have certain limitations. They cannot tell much about the content of the messages that are passing by, especially if they are encrypted. They are not useful for detecting, for example, if members of the internal network are leaking out corporate secrets. However, they can be very useful. Cheswick and Bellovin at AT&T claim that a firewall prevented the Internet worm from getting into their system.

3 Internet Protocol (IP)

IP host addresses are 32 bits long (though soon they will be 128 bits). Every machine on the Internet has a host address. There are also different classes of addresses:

Class C	$110\ \overbrace{network}^{21}\ \ \overbrace{host}^{8}$
Class B	$10\ \overbrace{network}^{14}\ \ \overbrace{host}^{16}$
Class A	$0\ \overbrace{network}^{7}\ \ \overbrace{host}^{24}$

Routing on the Internet is supported by:

1. *Routing Tables.* Each machine maintains various routing tables that enable it to figure out the destination of packets that come by. One security problem with routing tables is that they can be manipulated. If this happens, packets can be diverted ¿from their proper course by an adversary.

2. *Domain Name Service (DNS).* DNS translates symbolic names to numerical ones, and vice versa e.g *theory.lcs.mit.edu* to *Numerical Address.*

4 Transfer Control Protocol (TCP)

Packets going across the Internet have a source machine and a destination machine. There are various protocols implemented for transferring these packets. These include *ICMP (Internet Control Message Protocol)*, *UDP (User Datagram Protocol)* and *TCP (Transfer Control Protocol).* TCP is the one of most interest to users.

4.1 Ports

There are port numbers associated with the different network services. Port numbers below 1024 are usually the standard services (mail, ftp etc), whereas those above 1024 are for user-oriented services. Some typical port numbers and their corresponding service for TCP are:

Port 79	-	finger
Port 80	-	http
Port 25	-	smtp (mail)
Port 6000	-	X11 (X windows)
Ports 20, 21	-	ftp

A typical packet has the following attributes:

Type: TCP
From: Source IP address
From: Source port number
To: Destination IP address
To: Destination port number

These packets are not authenticated in any way.

4.2 Source routing

Packet routers try to find the shortest route for a packet that is going by. This means that sometimes a packet can be forced to take particular route. One implication of this is that an eavesdropper may be able to force packets to go by a certain machine, or to appear as though they are coming from a certain machine. However, this can also be used in a beneficial way, for example, to avoid potential problem areas, or untrusted parts of the network.

5 Packet Filtering

Firewalls usually have to deal with TCP or UDP packges. First we examine a typical TCP/IP session, and then see how a firewall might use packet filtering to limit the

Internet access of an internal network.

Figure 2 shows a typical TCP session. Port 80 is used, which means that this is an HTTP connection.

In the diagram:
1000 is a randomly generated sequence number
SYN means "synchronization"
ACK means "acknowledgement"
FIN means "finish"

A firewall needs to decide whcih parts of the transaction it will allow, disallow, or modify.

5.1 Example Packet Filter

Suppose a system wants to support email (and nothing else) between the Internal network and the Internet. Th packet filter can be made to only allow packets related to email to go through (note that there is still a potential security problem since some mail programs have bugs and can be used for other purposes e.g to execute shell commands).

A packet filter may have the following rule set:

¿FROM	ACTION	SOURCE	PORT	DEST	PORT	FLAGS
A	Allow	Our Hosts	*	*	25	

"FROM A" refers to the link A between the internal network and the firewall (see figure 1). It should be noted that it is not *guaranteed* that port 25 is for mail, though this is *usually* the case.

So far, this rule would allow the first packet i.e SYN(1000). To allow more access we add the following rules:

¿FROM	ACTION	SOURCE	PORT	DEST	PORT	FLAGS
Ch B	Allow	*	25	*	*	ACK
Ch A	Allow	Our Hosts	*	*	25	ACK

We need to consider whether these three rules allow email access as well as provide security from both inside and outside attacks.

One possible attack is *tunneling*. The firewall can be defeated if there is a cooperating pair, one on the inside of the system, and one on the ouside (on the Internet). The outside party can make requests on behalf of the inside one, e.g make a web request and then send it back to the inside user as email (to port 25). This is effectively giving the inside user web access.

5.2 A More Complicated Packet Filtering Example

Suppose the system also wants to allow ftp access to its users. Ftp uses two ports, one for control, and one for file transfer. Figure 3 shows a typical ftp session.

The danger here is that port X (usually a number greater than 1024) is opened from the outside. However, this can be switched around, and the ftp server can be requested not to open the connection, but allow the user to. This is what a packet filter would require. Figure 4 shows this sort of ftp connection.

There is still a potential security problem with the ftp connection. The internal users have the capability of connecting to any random port Y on the outside. Y may not necessarily be an ftp port number (e.g it could be a number greater than 1024). So users may be able to get access other than ftp.

6 Application-Level Gateways

Packet level filters have their limitations. An application level approach to filtering allows the contents of the packets to be examined in more detail. This is a more sophisticated way of doing filtering, and applies more intelligence to the system. Figure 5 shows a possible set up for this, with a bastion host sitting between two packet filters.

The bastion host understand the various Internet protocols (e.g ftp, http) better than the packet filters, and can be used to enforce a more sophisticated security policy. It has a host address both in reference to the Internet and in reference to the internal network. The bastion host can be used to implement an application-level gateway. Most sophisticated systems tend to have this combination of bastion host and packet filters. The bastion host can also be used to log connection attempts.

The following protocols are examined to see how an application gateway might be useful:

Gopher. Gopher supports UUencoding, in that it takes UUencoded files from the Internet. Some gopher programs copy the files in with the same permission bits as the original, which can pose security problems. The intelligence to recognize a UUencoded file can be placed in the bastion host, which can automatically disallow them.

Telnet. The bastion host can decide which other hosts can be connected to. The bastion host can also control the rate of data transmission of the telnet connection.

WWW. A firewall could be placed in a school so that no adult material is allowed in. The bastion host will need to understand labels. An application gateway might also be able to rewrite anchors so that url requests come back to it.

Another example is the use of *TCP wrappers*. These log connection attempts, then run off the request process. They can also do things like automatically fingering the machine that is sending the request, to find out who is logged on.

There is currently a library of tools for implementing firewalls, called TIS.

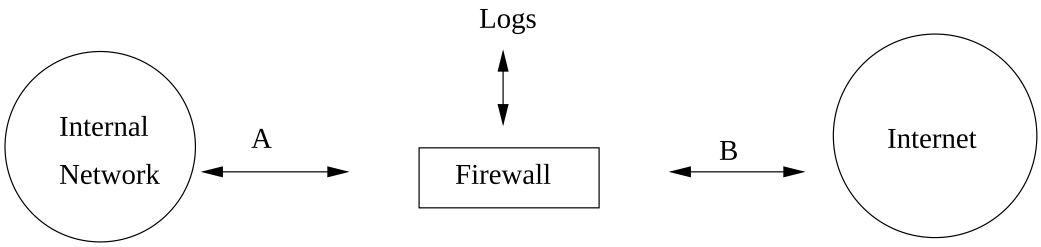

Figure 1: A firewall sits between the internal network and the Internet.

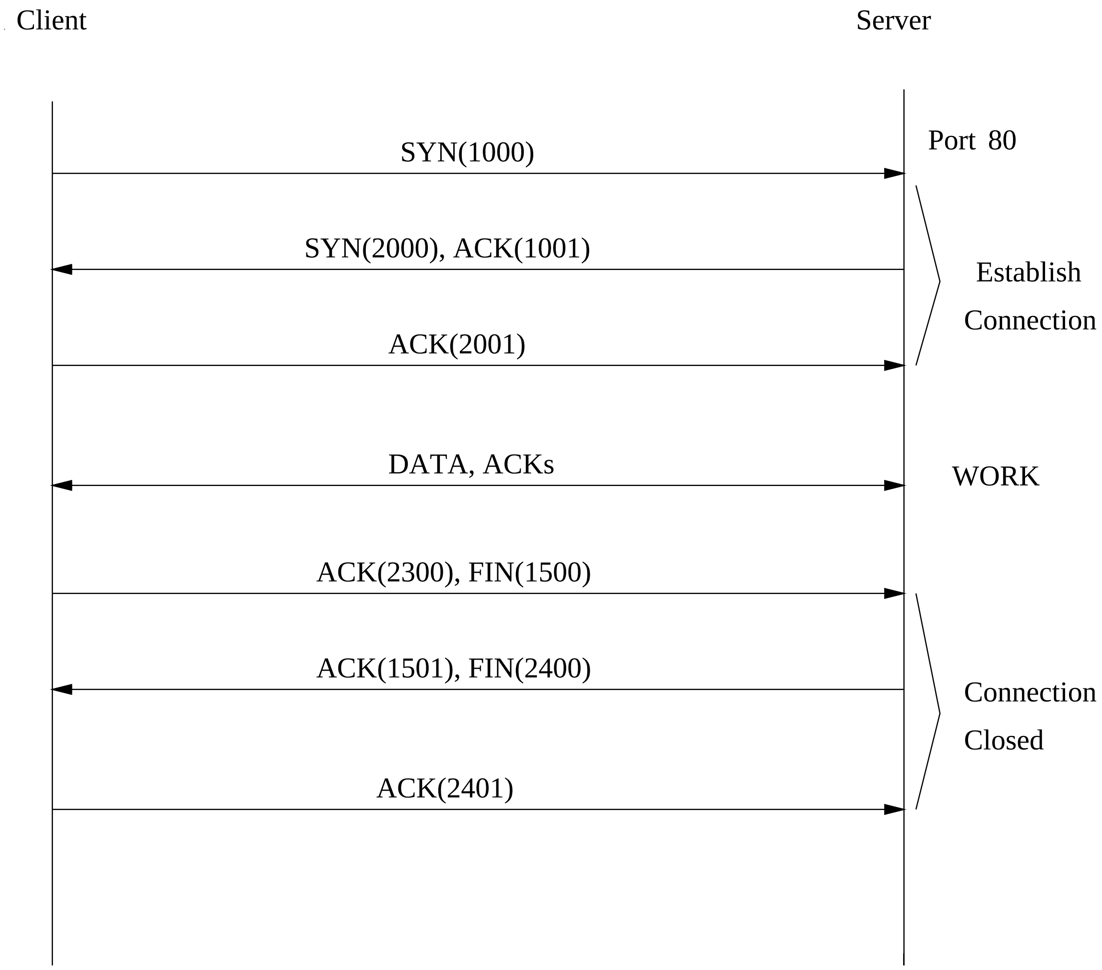

Figure 2: A typical TCP connection.

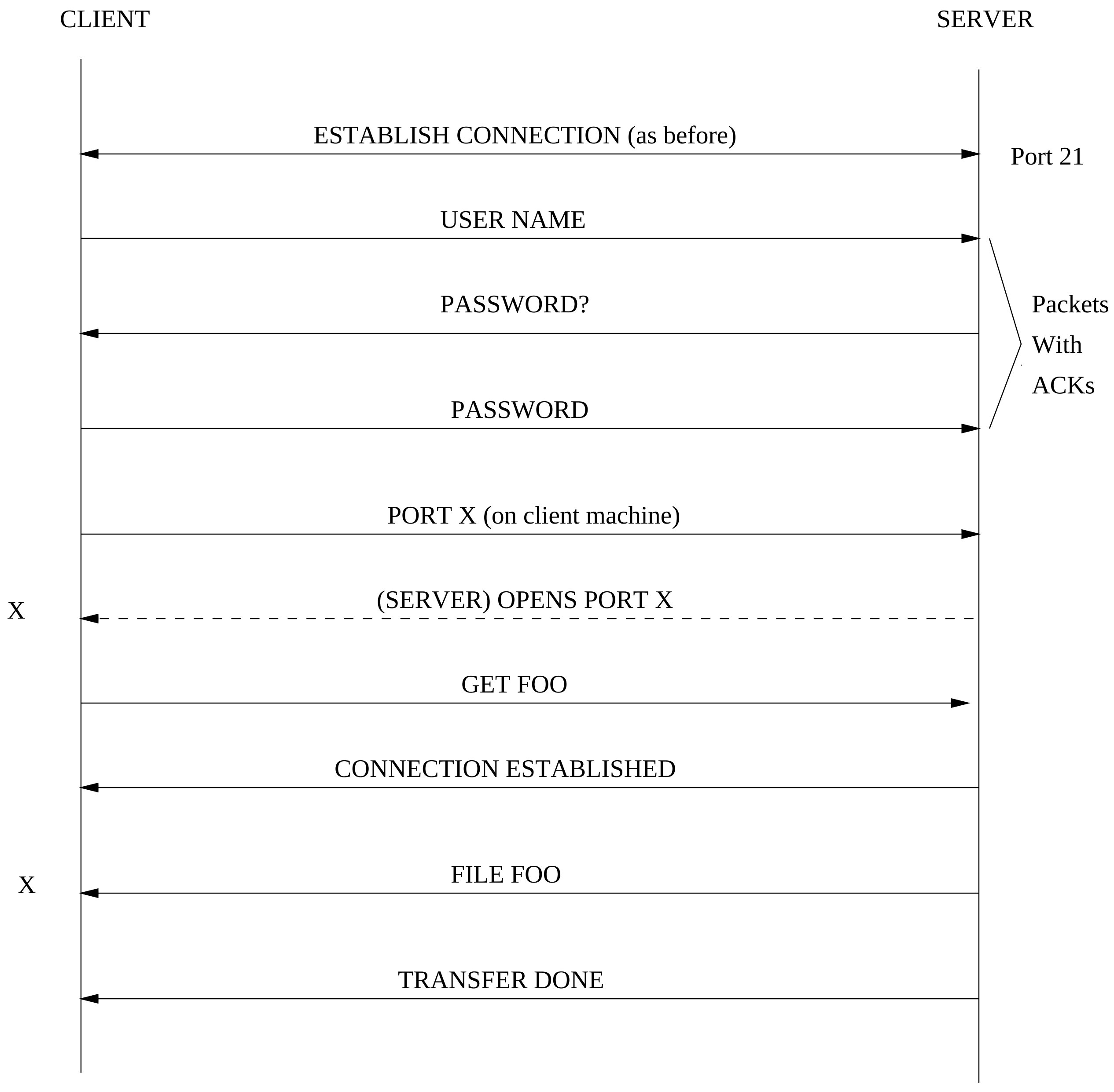

Figure 3: A typical TCP ftp connection.

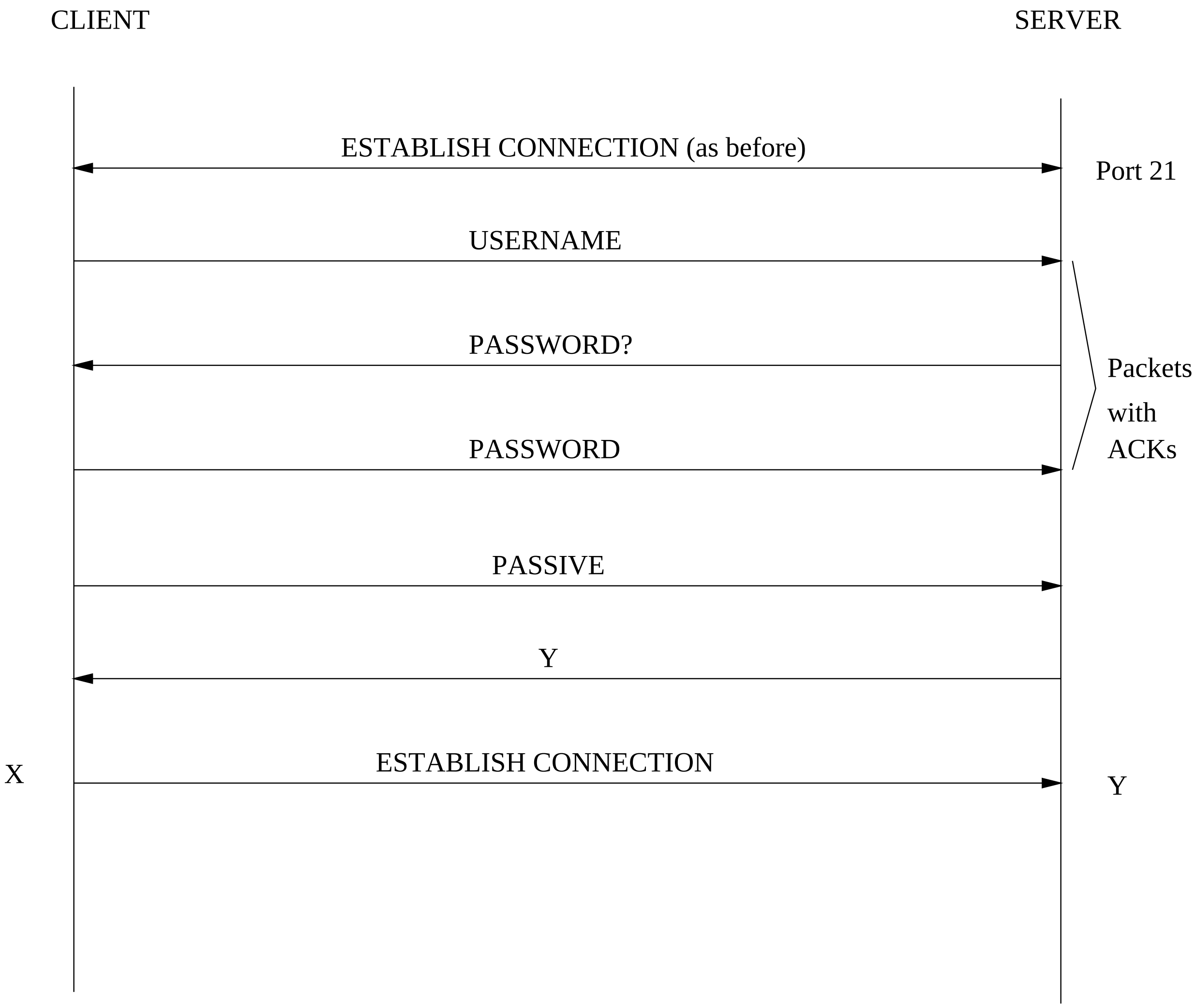

Figure 4: A passive TCP ftp connection.

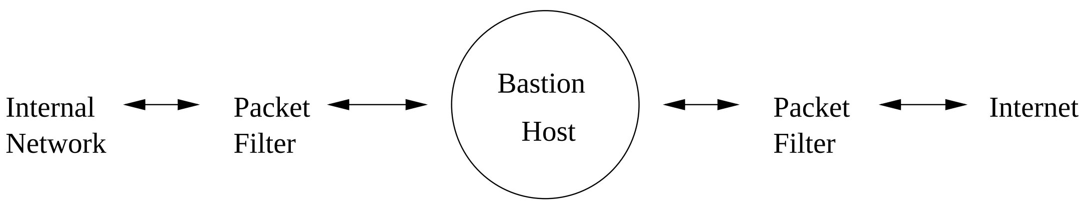

Figure 5: Using a bastion host.